In the Claims

Claim 1 (currently amended): A system comprising:

a recorder, including:

reading means for reading from an information carrier, a content of a medium mark, said content comprising a first bitpattern;

generating means for generating a second bitpattern according to a predefined relationship of with the first bitpattern;

encoder means for embedding a watermark representing the second bitpattern in user information to be recorded; and

recording means for recording the watermarked user information on the information carrier for storage;

the system further comprising:

a player including:

first reading means for reading the content of the medium mark, said content comprising the first bitpattern;

second reading means for reading the embedded watermark representing the second bitpattern from the user information;

verifying means for ~~verifying~~ establishing a verification of the relationship between the second bit pattern and the first bit pattern; and

enabling means for enabling playback of the recorded watermarked user information from the information carrier based on said verification.

Claim 2 (previously presented): The system of claim 1, in which the relationship includes a cryptographic function.

Claim 3 (previously presented): The system of claim 2, in which the relationship includes a one-way function.

Claim 4 (previously presented): The system of claim 1, in which the second bitpattern identifies the encoder means.

Claim 5 (currently amended): A recorder comprising:

reading means for reading from an information carrier, a content of a medium mark, said content comprising a first bitpattern;

generating means for generating a second bitpattern according to a predefined relationship with the first bitpattern; and

encoder means for embedding a watermark representing the second bitpattern in user information to be recorded; and

recording means for recording the watermarked user information in the information carrier for storage.

Claim 6 (previously presented): The recorder of claim 5, in which:

the recorder further comprises marking means for writing the medium mark on the information carrier; and

the generating means generate the first bitpattern from a seed according to a further predefined relationship.

Claim 7 (previously presented): The recorder of claim 6, in which the generating means generate the first bitpattern by combining a first part represented by a prepressed mark on a recordable information carrier and a second part generated from the seed.

Claim 8 (previously presented): The recorder of claim 6, in which the further predefined relationship includes a cryptographic one-way function.

Claim 9 (currently amended): An information carrier comprising:

a medium mark, wherein a content of said medium mark
comprises a first bitpattern; and

recorded user information encoded with a watermark representing a second bitpattern having a predefined relationship with the first bitpattern whereby the relationship between the second bitpattern and the ~~contents~~ content of the first bitpattern can be verified in a computer process.

Claim 10 (previously presented): The information carrier of claim 9, in which the first

bitpattern includes:

a first part identifying a source of the information carrier; and

a second part identifying the recorded information.

Claim 11 (currently amended): A player for an information carrier comprising:

first reading means for reading ~~the~~ a content of ~~the~~ a medium mark, said content comprising ~~the~~ a first bitpattern;

second reading means for reading ~~a~~ an embedded watermark representing a second bitpattern from recorded user information;

verifying means for verifying a predefined relationship between the second ~~bit pattern~~ bitpattern and the first ~~bit pattern~~ bitpattern; and

enabling means for enabling playback of ~~the~~ recorded user information from the information carrier based on said predefined relationship ~~verification~~.

Claim 12 (currently amended): The player of claim 11, in which the ~~verification~~ verifying means includes a cryptographic one-way function.

Claim 13 (currently amended): The player of claim 12, in which:

the verification means generate a verification pattern by applying a one-way function to the first bitpattern; and

the ~~verification~~ verifying means compare the verification pattern and the second bitpattern in order to verify the predefined relationship.

Claim 14 (previously presented): The system of claim 1, in which:

the relationship includes a one-way function;

the relationship includes a cryptographic function; and

the second bitpattern identifies the encoder means.

Claim 15 (currently amended) The recorder of claim 5, in which:

the recorder further comprises means for reading the first ~~bit pattern~~ bitpattern from the ~~record~~ information carrier;

the first bit pattern indicates a copy protection status of the ~~record~~ information carrier;

the relationship includes a cryptographic function;

the relationship includes a one-way function;

the second bitpattern identifies the encoder means;

the recorder further comprises marking means for writing the medium mark on the information carrier;

the ~~generator~~ generating means generate the first bitpattern from a seed according to a further predefined relationship; and

the ~~generator~~ generating means are arranged for generating the first bitpattern by combining a first part represented by a prepressed mark on ~~a recordable~~ the information carrier and a second part generated from a seed.

Claim 16 (currently amended): The information carrier of claim 9, in which:

the relationship includes a cryptographic function;

the relationship includes a one-way function; and

the second bitpattern identifies encoded user information ~~the encoder means~~.

Claim 17 (currently amended): The player of claim 12, in which:

the relationship includes a cryptographic one-way function;

the relationship includes a one-way function; and

the second bitpattern identifies the predefined relationship ~~encoder means~~.

Claim 18 (currently amended): The system of claim 1 in which the ~~second~~ medium mark is pressed in the information carrier during manufacture.

Claim 19 (currently amended): The system of claim 1 in which the watermarked user information is stored on the information ~~record~~ carrier in a different manner than the medium mark is stored, the user information writing means being insufficient for writing the medium mark on the information ~~record~~ carrier.

Claim 20 (previously presented): The system of claim 1, wherein said enabling means comprises an enabling switch.

Claim 21 (currently amended): The ~~system~~ player of claim 11, wherein said enabling means comprises an enabling switch.

Claim 22 (new): A system for copy protection of information recorded on an information carrier, the system comprising:

a medium mark on the information carrier containing a first bitpattern,

a recorder for embedding a watermark into a set of information data and for recording a watermarked set of information data on the information carrier, the watermark representing a second bit pattern having a predefined relationship to the first bitpattern, and

a player for verifying the relationship between the first bit pattern and the second bit pattern and for reproducing the watermarked set of information from the information carrier.

Claim 23 (new): The system of claim 22, wherein the predefined relationship comprises a cryptographic one-way function.

Claim 24 (new): The system of claim 23, wherein the second bitpattern is generated by applying a one-way function to the first bitpattern.

Claim 25 (new): The system of claim 22, wherein the recorder comprises encoding means for encoding a unique seed on the information carrier allowing the encoder means to be identified from the second bitpattern.

Claim 26 (new): A recorder for recording information on an information carrier containing a medium mark, the contents of the medium mark representing a first bit pattern, the recorder comprising:

generator means for generating a second bitpattern according to a predefined relationship between the first bit pattern and the second bitpattern,

encoder means for embedding a watermark in the information carrier, the watermark representing the second bitpattern, and

means for recording the watermarked information on the information carrier containing the medium mark.

Claim 27 (new): The recorder of claim 26, wherein the recorder further comprises marking means for generating the first bitpattern from a seed according to a further predefined relationship and for providing the medium mark on the information carrier.

Claim 28 (new): The recorder of claim 26, wherein the generator means are arranged for generating the first bitpattern by combining a first part represented by the contents of a prepressed mark on a recordable information carrier and a second part generated from a seed.

Claim 29 (new): The recorder of claim 27, wherein the further predefined relationship includes a cryptographic one-way function.

Claim 30 (new): An information carrier comprising:

recorded information, and

a medium mark, the contents of the medium mark representing a first bitpattern, the recorded information including a watermark representing a second bitpattern having a predefined relationship to the first bitpattern.

Claim 31 (new): The information carrier of claim 30, wherein the first bitpattern includes a first part identifying a source of the information carrier, and a second part identifying the recorded information.

Claim 32 (new): A player for reproducing information from an information carrier and comprising:

means for reading a medium mark from the information carrier, the contents of the medium mark representing a first bitpattern,

means for recovering a watermark from information read from the information carrier, the watermark representing a second bitpattern, and

verification means for verifying a predefined relationship between the second bitpattern and the first bitpattern, and

means for reproducing the information containing the watermark from the information carrier.

Claim 33 (new): The player of claim 32, wherein the verification uses a cryptographic one-way function.

Claim 34 (new): The player of claim 32, wherein the verifications means are arranged for generating a verification pattern by applying a one-way function to the first bitpattern and for comparing the verification pattern and the second bitpattern.

Claim 35 (new): The system of claim 22 wherein the medium mark is contained in a wobble of a track of the information carrier, the wobble representing the first bit pattern.

Claim 36 (new): The player of claim 32 wherein reproduction of information by the player is dependent upon the predetermined relationship as verified by the verification means.

Claim 37 (new): The recorder of claim 26 further comprising further encoding means for cryptographically scrambling the watermarked information using the first bit pattern before the watermarked information is recorded so that recorded information is scrambled.

Claim 38 (new): The system of claim 22 wherein the first bit pattern is a cryptographic key for de-scrambling recorded information to recover the watermarked information, and the second bit pattern is recovered from the watermark of the watermarked information.

Claim 39 (new): The recorder of claim 26, wherein the recorder further comprises means for reading the medium mark from the information carrier.

Claim 40 (new): The recorder of claim 26 wherein the recorder manufactures a disk by pressing.

Claim 41 (new): A recorder for recording information on a record carrier, comprising:

means for reading a medium mark from the information carrier, the contents of the medium mark representing a first bitpattern;

means for determining whether the information contains a watermark representing a second bitpattern that has a predetermined relationship with the first bit pattern; and

means for recording information dependent upon result of the means for determining.

Claim 42 (new): The player of claim 41 wherein the means for determining further identifies a verification pattern by applying a one-way function to the first bitpattern and comparing the verification pattern and the second bitpattern.